## Case 2:16-mj-00960-JS Document 30 Filed 02/14/17 Page 1 of 74

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH WARRANT 16-960-M-1 TO GOOGLE	NO.	) ) )	Misc. No. 16-MJ-960-1
IN RE SEARCH WARRANT 16-1061-M TO GOOGLE	NO.	) ) )	Misc. No. 16-MJ-1061
		) ) )	Philadelphia, PA January 12, 2017 1:02 p.m.

TRANSCRIPT OF HEARING
BEFORE THE HONORABLE THOMAS J. RUETER
UNITED STATES MAGISTRATE JUDGE

## **APPEARANCES:**

For the Government:

ANDREW S. PAK, ESQUIRE DEPARTMENT OF JUSTICE 1301 New York Avenue, N.W. Washington, DC 20530

MICHAEL L. LEVY, ESQUIRE JAMES A. PETKUN, ESQUIRE

ROBERT JAMES LIVERMORE, ESQUIRE ASSISTANT UNITED STATES ATTORNEYS UNITED STATES ATTORNEY'S OFFICE

615 Chestnut Street

Suite 1250

Philadelphia, PA 19106

For the Respondent, Google, Inc.:

TODD M. HINNEN, ESQUIRE PERKINS COIE 1201 Third Avenue Suite 4900 Seattle, WA 98101

WILLIAM A. DeSTEFANO, ESQUIRE TERRI A. PAWELSKI, ESQUIRE

STEVENS & LEE

1818 Market Street

29th Floor

Philadelphia, PA 19103

Audio Operator: CHRIS KUREK

Transcribed by: DIANA DOMAN TRANSCRIBING, LLC

P.O. Box 129

Gibbsboro, New Jersey 08026-0129

Office: (856) 435-7172 Fax: (856) 435-7124

E-mail: <u>dianadoman@comcast.net</u>

Proceedings recorded by electronic sound recording, transcript produced by transcription service.

(The following was heard in open court at 1:02 p.m.) 1 2 THE COURT: Good afternoon, everybody. 3 ALL COUNSEL: Good afternoon, Your Honor. 4 THE COURT: Please have a seat. Thank you. So before we begin I just want to ask both counsel, 5 do you want me to put this transcript under seal? Do you want 6 to think about it after the hearing to see what comes out? 7 8 Okay. Good. 9 MR. LEVY: It's one of those cases, Your Honor, where most of the filings up to this point have not mentioned. 10 There's one that does mention the name of an account and I'm 11 12 not sure that anybody's going to mention that. 13 THE COURT: And I don't think we need to get into those details in this hearing. 14 15 MR. LEVY: Yes. And I don't think we plan to do that today. 16 17 THE COURT: Yes. 18 MR. LEVY: So why don't we see where we are? 19 THE COURT: Okay. So let me put on the record, we're here because the 20 21 Government has filed motions to compel Google to comply with search warrants that were issued by this Court that have been 22 docketed at Number 16-960-M-1. 23 The second warrant was docketed at 16-1061-M. 24 25 Before we begin I'd like to have counsel identify

themselves for the record if they would please. And I'll 1 2 start with the Government first, please. MR. PAK: Good afternoon, Your Honor. Andrew Pak, 3 Trial Attorney with the Department of Justice, on behalf of 4 the Government. 5 THE COURT: Thank you, Mr. Pak. 6 MR. LEVY: Michael Levy, Assistant United States 7 8 Attorney. 9 THE COURT: Thank you, Mr. Levy. MR. PETKUN: James Petkun, Assistant United States 10 Attorney. 11 12 THE COURT: Thank you. MR. PETKUN: And Mr. Livermore is here in the event 13 14 we need him. 15 THE COURT: Right. Okay. 16 MR. PETKUN: Because he has an interest in one of 17 these --18 THE COURT: Right. 19 MR. PETKUN: -- matters. 20 THE COURT: Right. Mr. DeStefano. MR. DeSTEFANO: Good afternoon, Your Honor. 21 I'd like to introduce counsel who will be taking the 22 laboring oar here. It's Todd Hinnen from the Perkins Coie 23 firm in Seattle. And Mr. Hinnen has been admitted, I think by 24 25 prior order, pro hac vice --

THE COURT: Fine. Thank you, Mr. Hinnen. 1 2 MR. DeSTEFANO: -- for purposes of this proceeding. 3 THE COURT: Thank you, Mr. DeStefano. 4 THE COURT: Okay. Yes, ma'am. MS. PAWELSKI: Good afternoon, Your Honor. Terri 5 Pawelski with Stevens and Lee with Mr. DeStefano. 6 7 THE COURT: Okay. Great. Thank you very much. 8 Okay. The first thing we want to do is you want to 9 execute this stipulation, Mr. Levy? You had written that you 10 want to do that in open court. Do you want to do that first? 11 MR. LEVY: Yes. 12 THE COURT: I don't know if I have the original. 13 MR. LEVY: We've done that, Your Honor. THE COURT: Oh, you have? 14 15 MR. PAK: The stipulations have been executed. THE COURT: Okay. Do you want to hand that up and 16 we'll file it and make it part of the record? 17 MR. PAK: Absolutely, Your Honor. 18 19 THE COURT: Okay. 20 MR. LEVY: Your Honor, the stipulation applies to 21 both cases. There were some minor facts about what Google had provided that's different in each one, but the facts that 22 really govern the Court's decision are the same. 23 24 THE COURT: Okay. Great. 25 So, Mr. Hinnen, I'll address you first. Do you wish

Hinnen - Argument to present any evidence on behalf of Google? 1 2 MR. HINNEN: No, Your Honor, I don't. 3 THE COURT: Okay. And how about the Government, do 4 they wish to present any evidence at this time? 5 MR. PAK: No, Your Honor, we don't. THE COURT: Okay. So let me, if I could, I'll hear 6 from Google and I have some questions. 7 8 MR. HINNEN: Sure, that would be great, Your Honor. 9 Would you prefer I address you from here or --10 THE COURT: Whatever your preference is. MR. HINNEN: I'm comfortable here --11 12 THE COURT: Okay. MR. HINNEN: -- if that works for you, Your Honor. 13 Great. Thank you. 14 15 Your Honor, just way of background, Google receives 16 well over 25,000 pieces of legal process from Government agencies in the United States, Federal, State and local in 17 criminal matters every year. And Google's objective in each 18 19 case is do the same, to comply with the law as it applies to 20 that particular piece of legal process. 21 One of the laws that governs Google's response to such process is the law that we're here to discuss today, the 22 Stored Communications Act or the SCA. 23

And for purposes of this case the SCA governs the conditions under which a provider may disclose, or must

24

25

THE COURT: Okay.

disclose, information about its users or subscribers, including a section that provides specific types of legal process the Government may use to compel a provider to disclose such information.

In the 30 years since the SCA has been passed Congress has enacted a few minor amendments, but it has not overhauled or modernized the statute to keep up with the evolving technologies it governs or with the global communications networks that support those technologies.

And one of the things my client would like me to stress to the Court today is that the statute is in need of modernization and it sees that as the solution to the series of problems presented in both the Second Circuit Microsoft case and in the two cases that have brought us here today.

THE COURT: Was there an issue before <u>Microsoft</u>?

Were you -- were you complying with these subpoenas and -excuse me -- and/or search warrants even though your servers
were located outside of the United States?

MR. HINNEN: Before <u>Microsoft</u> we were, Your Honor -THE COURT: Okay.

MR. HINNEN: -- complying with them and there was not -- I would say <u>Microsoft</u> focused everyone's attention on data location in a fashion that it hadn't been focused on that before.

MR. HINNEN: Which is not to say that there weren't challenges and issues raised by the application of national law to a global network, the possibility of jurisdictional challenges and data being outside the jurisdiction of the Government -- whichever Government, the United States Government or another Government, that was trying to compel it.

THE COURT: I didn't mean to interrupt your flow.

MR. HINNEN: That's quite all right.

THE COURT: Go ahead.

MR. HINNEN: That's quite all right.

So despite the scope and importance of the SCA and its role in governing providers not only has it been amended relatively few times, but judicial opinions interpreting and applying the SCA are relatively rare as well for a 30 year old statute.

And as a result of that when a Circuit Court interprets and applies the statute the entities to which it applies, both the Government and providers, take notice.

For instance, the Second Circuit's decision in <a href="Warshak">Warshak</a> in 2010 which determined that a user has a constitutional right of privacy in its communications in the hands of a provider was immediately embraced by the providers, accepted by the Government and applied by Courts across the country, notwithstanding the fact that it was a Sixth Circuit

precedent.

So that brings us, Your Honor, to the <u>Microsoft</u> decision. And I'm sure the Court is well aware of it after reading the parties' pleadings, but in a unanimous decision last July the Court issued an opinion interpreting the SCA.

And the opinion is grounded in well established canons of interpretation and principles of law. And it decided that a search warrant issued under the SCA cannot compel a provider to produce data that is stored outside the United States.

At this juncture, Your Honor, there's no contrary precedent in any circuit in the country, nor am I aware of any contrary precedent in any District Court in the country, certainly not any published precedent. The Government can correct me if -- if the issue's been addressed in a sealed proceeding or that kind of thing.

THE COURT: That brings me to just one real quick question while its on my mind. Are there any other pending applications by the Government to compel Google to comply with your search warrants in situations like this that, first of all, are in this district?

And Mr. Levy's shaking his head, no. Okay.

MR. HINNEN: I agree with that, Your Honor.

THE COURT: And I don't -- are there any in the country where you've already argued and have, you know,

1 litigated this?

MR. HINNEN: There -- there are not, Your Honor.

There are other cases pending and arguments even scheduled in one of them, but you're -- you're the first, Your Honor.

THE COURT: Okay. All right. You may proceed.

MR. HINNEN: Okay. Thank you very much.

Just briefly to address some of the arguments set forth in the Government's briefing.

The Government argues and cites to several cases that an SCA warrant may have effect in another district in the United States.

And argues separately that under other legal frameworks different types of private companies can be compelled to produce business records that they store overseas.

Your Honor, both of those arguments are beside the point to the argument that we're here to address today which is whether a warrant issued under the SCA is effective in compelling a service provider, the specific type of entity that the SCA governs, to produce documents that are stored overseas. And, as I mentioned, to that specific question only the Second Circuit has so far spoken.

Just one other argument in the Government's briefing to address before I -- before I go on.

The Government also argues that a treaty ratified 1 2 some 20 years after passage of the Stored Communication --3 THE COURT: And the Second Circuit didn't address 4 that argument at all? 5 MR. HINNEN: It did not address it. THE COURT: I don't know if it was raised, but it 6 may not have been raised. 7 8 MR. HINNEN: I don't believe it was raised. 9 THE COURT: Right. MR. HINNEN: Yes. I think it is raised maybe on the 10 motion for reconsideration. 11 12 THE COURT: Right. MR. HINNEN: In any event, Your Honor, I think it 13 strains credulity to suggest that congressional intent in 1986 14 15 can be determined from a treaty ratified by Congress in 2006. 16 THE COURT: Well, they do cite to some cases that 17 say that you can look at subsequent actions of Congress to determine their intent in prior legislation. They had some 18 19 cases. 20 MR. HINNEN: Sure, I understand that, Your Honor. 21 THE COURT: Right. MR. HINNEN: And, of course, you know, Congress has 22 23 amended the SCA minorly several times, including since 24 September 11th.

And the easiest way for Congress to make clear that

25

the SCA applies to data stored outside the United States would
be to say that the SCA applies to data stored outside the
United States or regardless of where in the world the data is
stored or something like that, so --

THE COURT: Okay.

MR. HINNEN: -- I certainly take the point, Your Honor.

Google's response to the <u>Microsoft</u> decision has been two-fold.

First, consistent with its principle approach to responding to legal process in all instances Google sought diligently and in good faith to comply with the law.

And, in fact, as the stipulation handed up before the parties -- by the parties just before argument began it indicates that Google has produced all of the data that is within the scope of the warrants that it has been able to determine are inside the United States.

THE COURT: Let's -- let me stop you there. Let's -- in your affidavit -- you filed an affidavit initially and the words you used were kind of nebulas or ambiguous. And I don't mean you intentionally did that, but you had said in there you could not confirm -- Google could not confirm that these emails, contents, attachments, whatever, were outside the United States.

I think you terminated -- you said -- you confirmed

that they weren't in the U.S. or weren't stored in the U.S. 1 2 What was the word you used? MR. HINNEN: I believe, Your Honor --3 4 THE COURT: Maybe you can correct me. 5 MR. HINNEN: -- what we said is that we produced everything we could confirm was --6 7 THE COURT: Right. MR. HINNEN: -- stored in the United States. 8 9 THE COURT: Could confirm. MR. HINNEN: Correct. 10 THE COURT: Okay. So do you know the things that 11 12 were asked for in the warrant that you didn't produce, do you know where they are stored, in what country? 13 MR. HINNEN: Well, Your Honor, the --14 15 THE COURT: Wherein, in Microsoft the evidence was 16 clear that they were in Ireland --17 MR. HINNEN: Yes, Your Honor. 18 THE COURT: -- in a server, but you --19 MR. HINNEN: And --20 THE COURT: Go ahead. 21 MR. HINNEN: -- the Microsoft network is a little different I think that the Google network. 22 23 THE COURT: Yes. 24 MR. HINNEN: The challenge with answering the 25 Court's question, and I don't intend to dodge it, but the

Challenge with answering the Court's question is that Microsoft's network is both distributed and dynamic and the network moves data when it feels that it's -- will maximum several network objections -- user experience, prevent latency, it spreads data to establish security and that kind of thing.

So although Google can -- the network always knows where every piece of data is. If it didn't the services wouldn't work and when Mr. Pak logged on to his Gmail account he wouldn't be able to access his Gmail account.

The question is with respect to the large variety of services that Google offers on that network, and there are tens if not hundreds of such servers -- services, Gmail being just one of them. The question is -- is whether Google has the capability to render to a human user that data at any particular point in time.

And, as Your Honor has already explored, prior to the <u>Microsoft</u> case data location was not a big focus necessarily of the SCA and it certainly wasn't a focus of --

THE COURT: The Internet providers.

 $$\operatorname{MR}.$$  HINNEN: In this sense of the Internet providers.

THE COURT: Right.

MR. HINNEN: And so Google has endeavored since the passage -- the handing down of the Microsoft opinion to

develop tools that will allow it to query its network and determine where data is at any given time and it has those tools with many of its -- with respect to many of its services.

And that's why in these cases Google has been able to produce one set of data to the Government and then make a supplemental production when a tool was completed and they were able to determine the location of that data and produce the data that was located in the United States.

But at any given time it may be true that not only is the data -- not only can the data move frequently, but what we would think of as a specific file, a specific document, stored in docs or on drive, may be split up into different parts and stored in different data centers in different jurisdictions.

THE COURT: So some of the -- I'm just summarizing.

I think I understand what you're saying that the content of an email and whether it could be the subject, heading, the email address, the actual contents or attachments, there's various shards I guess is the terminology that's been used, they could be in multiple countries?

MR. HINNEN: That's correct, Your Honor.

THE COURT: Servers in multiple -- located within different countries?

MR. HINNEN: That's correct, Your Honor.

Δ (

8 9

And in many cases the manner in which that is accomplished is different with respect to different services, sometimes it's different with respect to the body --

THE COURT: Right.

MR. HINNEN: -- of an email than it is for the attachment of an email.

THE COURT: So if I deny the Government's motion to compel what, if anything, can the Government do to obtain this information since they can't get it if I rule that way and the way you want me to apply the law from Google?

MR. HINNEN: Yes, that's a great question, Your Honor.

I mean, I think the best answer and I'm -- not at all to be clever, but I think the best answer is that the Government can work to reform the statute and address these issues which didn't exist in 1986 and provide a statutory framework that speaks to them expressly.

THE COURT: But what do you -- what do you say to the Government, and I'm not sure they explicitly made this argument, but if you set up a system -- and I'm not saying you intentionally did this. I'm not saying Google intentionally made it impossible to comply with a lawful warrant -- that you should be allowed to do that and leave the Government without a remedy.

MR. HINNEN: Well, first of all, I guess, Your

Hinnen - Argument 1 Honor --2 THE COURT: It strikes me as a little bit absurd. MR. HINNEN: Well, so several responses, Your Honor. 3 4 First, thank you for acknowledging that Google did 5 not intentionally do that. THE COURT: No, no, and I'm not describing that to 6 them. 7 8 MR. HINNEN: And, in fact, Google has worked since the <u>Microsoft</u> case to -- to try and make sure that that's not 9 10 the case. But I think it's a situation that arises -- it's a 11 12 situation that arises particularly with respect to digital 13 evidence, but not uniquely. It's always been the case that the Government has 14 15 been involved in investigations and data has been outside a 16 district or outside the United States and the Government has 17 had to resort to other measures to try and obtain the data. 18 There are such measures. The Government can try and 19 rely on the Mutual Legal Assistance Treaty or the Cybercrime 20 Convention that's --21 THE COURT: But they can't do that in this case with 22

Google.

MR. HINNEN: -- that's cited in its briefs.

23

24

25

THE COURT: Right? Can -- they can't do it with -they can't utilize those devices with respect to Google?

8 9

MR. HINNEN: With respect to content, Your Honor, it may be difficult to do that because what essentially -- well, not to prejudge how the Government might try and go about doing that -- and perhaps the Government has figured out a way to do that -- but there might be challenges to that, Your Honor.

So it is possible that there will be situations in which content stored overseas is not accessible to the Government under the rule announced by the Second Circuit unless and until the statute is reformed and modernized to address that issue.

THE COURT: Let's just talk briefly about subpoenas.

Is it your position that there's no distinction between a search warrant and a subpoena?

So, as you know, the Government cited many cases, many of them from the Third Circuit, even the Marc Rich case from the Second Circuit, where the Government can obtain records from someone living domestically in the United States even though those records are stored outside the United States' jurisdiction and compel them to produce those records.

The Second Circuit in their opinion when the Government made that argument they kind of -- how do I want to say it -- I don't think they addressed that squarely.

The Second Circuit, if I recall, made a distinction between when the custodian is a third party as opposed to the

Hinnen - Argument actual possessor or owner of the documents. Although there 1 2 are cases, and the Government cites them, that don't make that 3 distinction. What's your position if the Government subpoenaed 4 5 Google under the other provisions of the Act where the data was older than 180 days or whatever, would you have to comply? 6 MR. HINNEN: You know, Your Honor, I don't think 7 8 this case presents that issue. 9 And I don't think that a subpoena would be regarded as sufficient to provide content. I think Google would argue 10 that in the wake of Warshak if the Government were seeking 11 content it needed a warrant in order to get that content. 12 13 THE COURT: Did you think the Second Circuit decided that and made -- to sit that holder or did they avoid it as I 14 15 think they did? MR. HINNEN: I think they -- they were focused on 16 17 the warrant in front of them, Your Honor. 18 THE COURT: Right. 19 MR. HINNEN: And I think they relied to some degree on the use of the term of art warrant in the Stored 20 21 Communications Act and the historic practice and --22

THE COURT: And just stuck to the -- the Rule 41 and warrant?

23

24

25

MR. HINNEN: Correct. Yes. I mean, the debate, as Your Honor has put your finger on, is whether an SCA warrant

Hinnen - Argument is more like a probable cause subpoena --1 2 THE COURT: Right. MR. HINNEN: -- or like a traditional search 3 4 warrant? And the Second Circuit decidedly came down on the -on the latter side. 5 THE COURT: Okay. Now, I'd like you to just talk 6 for a minute about -- let's talk about the presumption against 7 8 extraterritorial applications. 9 So I understand that the Supreme Court in several cases has labeled that as a canon of statutory construction. 10 Is it your position that it has to be applied at all 11 12 times to any -- any time the Court construes an act of 13 Congress? Or is it like any canon of statutory construction, 14 15 it's just an aid that can be used to determine the intent of 16 legislation and like any aids it's not exclusive, it doesn't 17 have to always be applied? MR. HINNEN: I think, Your Honor, there's a 18 19 hierarchy and sequence of tools that a Court uses in trying to 20 construe the meaning of a piece of legislation --21 THE COURT: Right. MR. HINNEN: -- beginning with the text itself and 22 that -- that canons fall somewhere in -- in that -- in that 23 24 litany.

I think that in a case that involves arguably the

25

extraterritorial application of a statute a Court would be remiss if it didn't grapple with the presumption against extraterritoriality.

THE COURT: Okay. Let's talk about the first step of the application of the presumption under <u>Morrison</u> and the <u>Nabisco</u> case.

I think the Government -- and I'll hear from the Government in a minute -- but I think the Government would concede, as they apparently conceded before the Second Circuit, that there is -- the Stored Communications Act does not explicitly or make clear in the Act that it applies extraterritorial. I don't think that's the issue that I need to deal with. I think that's a given given the history of the litigation.

I think the crucial issue here is the second step.

And that requires me to focus on the purpose of either the statute or section within the statute.

The Government has made that argument, as I know you're aware, that they believe the Second Circuit erred under <a href="Nabisco">Nabisco</a> and even under <a href="Morrison">Morrison</a> in that they looked at this statute as a whole and determined that the focus -- the primary focus was privacy rather than looking at it section by section.

And under 2703(b), I believe it is, that section deals with disclosure and that in analyzing it in that way

it's clear that really what we have here is a domestic 1 2 application, not an extraterritorial application, especially 3 when you think about the architecture of Google. 4 Everything here -- you had said in your affidavit or 5 in your -- excuse me, in your stipulation, that this only can be accessed by people working for Google in the United States. 6 It can't be accessed overseas, is that right? 7 8 MR. HINNEN: It can't be accessed for this purpose 9 by people authorized to produce records in response to legal 10 requests. THE COURT: Right. 11 12 MR. HINNEN: That's correct, Your Honor. THE COURT: What is your position on the 13 Government's argument that the Second Circuit erred by not 14 15 analyzing it section by section as opposed to an overall view 16 of the statute? MR. HINNEN: You know, Your Honor --17 18 THE COURT: And you saw that argument, right? 19 MR. HINNEN: I did. THE COURT: Yes. 20 21 MR. HINNEN: Absolutely. I'm not sure Google has a position on -- on that 22 23 argument. I think the Stored Communications Act clearly 24

addresses both privacy and the appropriate mechanism by which

25

law enforcement can compel information.

I think even with respect to a particular section or provision it may be an oversimplification to say that it focuses on one to the exclusion of the other.

I think the reason that 2703 is structured the way it is providing the strongest procedural and substantive protection for the data that is the most private suggests that even though it's concerned with the issuance of legal process by the Government and -- and the Government's access to data, it's also concerned with -- with customer privacy even in that provision.

And I think customer privacy is the -- is what pervades the statute, 2703, as an exception to the prohibitions on disclosure in 2701.

And so I think it's very -- it's a very difficult question, Your Honor.

THE COURT: And even I think Judge Lynch when you read his concurring opinion he struggled with that.

MR. HINNEN: I think that's right.

THE COURT: Right.

MR. HINNEN: And not to go back to my dead horse,
Your Honor, but this really is why these challenging policy
issues that aren't unique to these parties and aren't unique
to these cases should be addressed by Congress and the statute
should be reformed so that there's a clearer answer.

I know that doesn't help us here today, but that really is -- Google's position with respect to this is that we should fix this problem rather than keep struggling with an outdated statute --

THE COURT: Okay.

MR. HINNEN: -- the terms of which don't address this.

THE COURT: Let me ask you another way, if I could?

So if I do order Google to provide this -- all the contents of the emails, we're dealing with I think it's undisputed here in both cases, we have a subject of a criminal investigation who resides in the United States.

We have emails that as far as I can see, and as far as the record shows, were emails that were generated solely domestically. In other words, it wasn't emails from this country to someone in a foreign country. The crime itself was one that occurred exclusively in the United States.

The provider here, Google, has easy access in the United States to disclose these emails through it's personnel who reside in the United States.

Tell me the extraterritorial application that would be implicated or would be applied if I order you to produce these emails given the record I have here today which is apparently a little bit different than the record before the Court in <a href="Microsoft">Microsoft</a>.

1 MR. HINNEN: Sure, Your Honor.

I think following the Second Circuit's precedent the extraterritorial application would be <a href="Microsoft's">Microsoft's</a> -- Google's search of its foreign data centers to identify where responsive data in those data centers is and the seizure of that data from those data centers to bring it back and repatriate it as part of its role in assisting the Government in executing the warrant.

THE COURT: I know you use the language that

Microsoft said that that -- the seizure is the actual

retrieving of the data, but really where does -- I mean, the

Government has argued, and the Magistrate Judge Francis had

said in his opinion, that really the search occurs in the

United States.

That's where the disclosure -- the disclosure doesn't -- let me put it this way, the disclosure doesn't happen overseas, the disclosure happens in the U.S. You'd have to agree to that?

MR. HINNEN: I would, Your Honor.

THE COURT: Okay. All right. Is there anything else you want to -- you want to talk about?

I have a couple of other questions. Is there anything -- I kind of interrupted your argument, so --

MR. HINNEN: No, Your Honor. I think we really covered what I intended to cover in my opening. Thank you.

Hinnen - Argument THE COURT: Okay. Can I ask you two other questions 1 2 though before --3 MR. HINNEN: Yes. 4 THE COURT: And this is -- this is these other 5 issues you raised. The first issue was the overbreadth. I noticed that 6 you made the argument in the first warrant, but the second 7 8 warrant I'm not sure you put that in your brief. Are you 9 abandoning that argument after the Government said you didn't 10 have standing to raise that? 11 MR. HINNEN: I don't think we're abandoning it, Your 12 It is Google's position that a warrant that encompasses all data on all services is overbroad. 13 That the Government has an obligation to identify 14 15 with particularity which services it thinks store data that 16 constitute evidence of the crime that it's investigating. 17 I do think that the Government and Google have 18 reached a point in that -- in this case where that issue may be moot. 19 20 Google has produced all data, except that data which is subject -- arguably subject to the Microsoft rule. And 21 there's not a class of data that's left for the Government and 22

Google to argue about with respect to whether it's subject to an overbroad subpoena.

23

24

25

THE COURT: So is this a moot argument now?

Case 2:16-mj-00960-JS Document 30 Filed 02/14/17 Page 28 of 74 Hinnen - Argument other words, you're saying you produced everything in all the 1 2 accounts? 3 MR. HINNEN: Yes. You know, I think this goes --4 this goes to the practice of executing or responding to --THE COURT: You're looking at the future? 5 MR. HINNEN: -- these warrants. 6 Well, it goes -- it goes to it in the sense, Your 7 8 Honor, that the Government's often in the position of coming 9 in and having to swear out a warrant in a situation where it may not have a complete understanding of a provider's network 10 architecture, its data storage practices or even the mechanics 11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

of its services.

And it then relies on Google, as compelled by the warrant, to help determine what those facts are and to execute the warrant in a reasonable and lawful manner in light of those facts.

So in this particular case I think the warrant was overbroad -- Google thinks that the warrant was overbroad as issued because it swept in every service and every piece of data associated with every -- every service.

But through the standard process of execution that applies with respect to SCA warrants the Government and Google have arrived at an agreement with respect to what data they intended it to apply to. Google's produced that data and I think that point is largely moot now.

Hinnen - Argument The other thing I would say, Your Honor, is if you 1 2 grant the relief Google requests it will certainly moot that 3 point. 4 THE COURT: All right. And the other issue is on the disclosure order -- non-disclosure order. 5 MR. HINNEN: Correct, Your Honor. 6 THE COURT: I'm hoping we can work something out 7 8 here today so I can concentrate on the bigger issue. 9 What period of time do you think is appropriate? You're kind of acknowledging that there is a validity to 10 having a non-disclosure order. I think your only argument is 11 12 that the order I entered didn't have a set time period when 13 you were allowed to disclose it. Is that essentially --MR. HINNEN: Yes, Your Honor. 14 15 And that's our argument here today. There's -- and 16 there's litigation proceeding before the Western District of 17 Washington as to whether 2705 is unconstitutional on its face. You know, I think Congress in the USA Freedom Act 18 19 20 21

about a year and a half ago established a framework with respect to NSL's in which the standard period for nondisclosure was a year and the Government was required to come back to Court and say --

THE COURT: You cited that case.

MR. HINNEN: Yes.

22

23

24

25

THE COURT: Yes.

MR. HINNEN: And say, you know, Your Honor, the 1 2 conditions for non-disclosure still exist and the Government would still suffer -- suffer one of the five statutorily 3 4 enumerated harms if there were disclosure, so please extend the non-disclosure order for another year. 5 THE COURT: How about five years? That's the 6 statute of limitations for Federal crimes if they don't indict 7 8 by that time. 9 MR. HINNEN: You know what, what the statute -- what 10 the statute --THE COURT: If I --11 MR. HINNEN: -- directs is for the Court -- the 12 13 Court to enter an appropriate period of time. THE COURT: Well, if I enter an order -- if I amend 14 15 this order and make it five years are you still going to pursue this argument? 16 17 MR. HINNEN: I don't know, Your Honor. I think it's 18 difficult to prejudge -- to prejudge the response to the --19 THE COURT: No, no, I mean, I'm trying to get your agreement now on this argument. 20 21 MR. HINNEN: I understand. THE COURT: If I can get Mr. Levy to agree that we 22 23 can do a five year order locking, put that aside and 24 concentrate on these more weighty issues that are, obviously,

25

more troublesome.

Case 2:16-mj-00960-JS Document 30 Filed 02/14/17 Page 31 of 74 Hinnen - Argument MR. HINNEN: I would have to confirm with my client, 1 2 Your Honor, but I would think that a five year term might be 3 something they would seriously consider. 4 THE COURT: Okay. Let me ask you one other question 5 I forgot to about the -- the presumption against extraterritorial application. 6 I'm looking at my notes for the -- as you know, the 7 8 Courts are concerned and the reason they apply this 9 presumption is they're trying to avoid conflicts between the U.S. and foreign nations. I think the word they use is 10 friction. 11 Given the fact that Google stores these email 12 contents in various countries all over the world -- in fact, 13 you quite candidly told me you're not even sure what country 14 15 these are in -- what friction with foreign countries should the Court be worried about should the Court grant the 16 17 Government's relief here? 18 19

MR. HINNEN: I think the potential friction, Your Honor, is the assertion of jurisdiction by a foreign country over data stored within its borders and it's --

THE COURT: They don't even know about this data, though. Come on, they don't even know about it.

20

21

22

23

24

25

MR. HINNEN: They know -- they know that there are data centers -- centers in their country where -- where providers store data.

Hinnen - Argument And it's an -- it's not a hypothetical -- it's not a 1 2 hypothetical issue, it's an issue with respect to which 3 several foreign sovereigns have passed legislation. Russia has a data localization statute. Germany has a data 4 5 localization statute. THE COURT: Which says what? What's a data 6 localization statute? I'm not sure. 7 8 MR. HINNEN: That says essentially if you're doing 9 business in Germany with respect to German citizens you must store the data relating to that business here in Germany or in 10 Russia or at least store a --11 12 THE COURT: But that's not the facts of our case. 13 MR. HINNEN: -- a copy there. THE COURT: We don't have -- we don't have foreign 14 15 citizens involved in this criminal investigation. MR. HINNEN: No, Your Honor, but we're -- we may be 16 17 talking about a -- we certainly are talking about a statute 18 that applies much more broadly than these particular cases. 19 20 21

22

23

24

25

The one other point I'd make is that, you know, historically that's been a big issue. And the Government reaching across international boundaries in order to obtain data in support of an investigation is something that Court's have -- the <u>Gorshkov</u> case in the Western District of Washington in which a couple of FBI agents reached back to the data stores of a hacker in Russia and obtained his hacking

Pak - Argument tools as evidence to prosecute him. He had been lured to the 1 2 United States. 3 And then that was -- as a result of that the Department of Justice implemented a practice of checking with 4 the Office of International Affairs before companies proceed 5 in that respect. 6 It also requires Assistant U.S. Attorney's to check 7 with the Department of Justice before they proceed even with a 8 9 regular Bank of Nova Scotia subpoena if it's going to implicate the interests of foreign -- foreign countries. 10 11 So I think in the absence of a clear expression by 12 Congress on this issue and Congress' ability to weigh those comity issues amongst the various other policy issues 13 implicated by the SCA and the Second Circuit's interpretation 14 15 of it, those are -- those are real issues. 16 THE COURT: Okay. Thank you very much. 17 I'll hear from the Government. Mr. Pak, do you want 18 to argue for the Government? 19 MR. PAK: Yes, Your Honor. 20 THE COURT: Go ahead. 21 MR. PAK: May I use the podium? THE COURT: Sure, absolutely. 22 MR. PAK: So Your Honor's obviously familiar with 23 our briefing with respect to the two search warrants. 24

But I wanted -- what I wanted to do is to go over

25

the four main points that we have as to why we think the <a href="Microsoft">Microsoft</a> decision should not be applied.

And, first, I'd like to address that in the context of what Mr. Hinnen is suggesting which is a legislative fix here. Obviously, this Court should first look at whether the statute itself needs fixing before saying that that should be the option that is pursued.

THE COURT: Right.

MR. PAK: And our first --

THE COURT: And just because the Congress at the time in 1986 couldn't envision the growth of the Internet does that -- does not necessarily preclude the Court from trying to discern the Congressional intent in interpreting the statute?

I mean, it seems like the argument -- even some -- some of the Judges in the Second Circuit said well, just -- we have to throw up our hands since they didn't envision this in the first place and, obviously, we can't construe it.

But is -- are there cases by the Supreme Court that says, look, even though Congress may not have thought of a particular problem, Court's can still construe the statute to try to address that problem?

MR. PAK: Absolutely, Your Honor. And that is the line of cases with respect to <u>Red Lion Broadcasting</u>, <u>Bell versus New Jersey</u>, as well as <u>Schor</u>, where the Supreme Court has actually looked at subsequent legislative history, so to

Pak - Argument speak, post-enactment action by Congress to interpret an 1 2 original --3 THE COURT: You cited them, right? 4 MR. PAK: Yes. 5 THE COURT: Yes.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

MR. PAK: Additionally, Your Honor, what's relevant in looking at the Stored Communication Act is the framework that it provides. And that framework provides in personam power to Courts to provide -- to require certain providers to produce information.

That in personam power is in a very relevant way distinct from a Court's traditional in-rem power to issue Rule 41 search warrants.

And the Microsoft Court failed to recognize that distinction, but that distinction is incredibly relevant because there is a wide variety of case law with respect to the scope of a Court's in personam power.

So even if Congress wasn't thinking about a provider such as Google in 1986, they provided a framework against the backdrop of common law and Court's can obviously look at that and that is another canon of statutory construction in determining what the SCA does.

And that's -- and the reason that distinction is relevant, Your Honor -- I think I'd like to take a step back and just talk about the type of data that's at issue here

which is essentially --1 2 THE COURT: Let me stop you though. 3 MR. PAK: Yes. 4 THE COURT: The canon instruction says you can look at the common law at the time that the statute was enacted. 5 What -- did you have any authority in your brief on that? I 6 don't recall that. I know you kind of make that point. 7 8 MR. PAK: I believe -- I believe there is a case on 9 that that we cited. I don't have that --10 THE COURT: Okay. MR. PAK: -- particular citation handy. 11 12 THE COURT: And the common law being it's the -- the general power the Court's have to order someone to produce 13 14 documents that are stored overseas? 15 MR. PAK: Yes, Your Honor. 16 THE COURT: Okay. 17 MR. PAK: In fact, it's such a longstanding principle that not only do we cite the Third Circuit cases, 18 but in Footnote 3 to both briefs --19 20 THE COURT: Right. 21 MR. PAK: -- we cite cases from all -- from many Circuits, as well as District Courts. And there's even a 22 23 restatement that says as much and the rule there --THE COURT: Mr. Pak --24 25 MR. PAK: Yes.

Case 2:16-mj-0096

THE

say because it

that the Second
the Marc Rich
cases -- Marc
possessor of the party custodian

held in the --a subpoena.

THE

critical, but

14

15

16

17

18

19

20

21

22

23

24

25

THE COURT: -- I want to hear everything you have to say because it's important, but what about this distinction that the Second Circuit made when they tried to distinguish the Marc Rich case? They said, well wait a minute, those cases -- Marc Rich dealt with actually the owner or the possessor of the documents and here we're dealing with a third party custodian.

And the other thing is they said no case is ever held in the -- under the Stored Communications Act you can use a subpoena. Can you address that a little bit?

MR. PAK: Yes, absolutely, Your Honor.

THE COURT: I mean, the Second Circuit, not to be critical, but it seemed to me they didn't really address that head on.

MR. PAK: They didn't, Your Honor.

Second Circuit addressed <u>March Rich</u> it said, look, <u>Marc Rich</u>,

<u>United States versus Bank of Nova Scotia</u> that is the law of subpoenas. Right? And it even had a section entitled the law on subpoenas and they're relevant.

I think the problem with their analysis is that it's not the law on subpoenas. Sure, those cases involved subpoenas, but the law that the Court's were applying was the scope of a Court's power in personam to compel a party before it -- even a non-party in a case -- to produce information.

Pak - Argument So they needed to look at the rationale behind those cases as 1 2 opposed to just dismissing them on law on subpoenas. Number two, Your Honor, if you look at the cases in 3 4 our Footnote 3, we have cases that involve not only the use of 5 subpoenas --6 THE COURT: Right. MR. PAK: -- but discovery, other situations where 7 8 the basis of a Court's power is in personam over the person, 9 as opposed to in-rem over a piece of property. THE COURT: And you also have cases where a third 10 party custodian is involved as opposed to the actual owner of 11 12 the records. 13 MR. PAK: Absolutely, Your Honor. THE COURT: Right. 14 15 MR. PAK: And here's the other problem with the logic that the Second Circuit used I think in talking about 16 17 the Bank of Nova Scotia. The Court there said well look, here's the 18 difference -- the difference here is the provider is merely a 19 caretaker for somebody else's documents. 20 21 However, Marc Rich and a lot of these other cases 22

that we cited deal with subpoenas directly to somebody that may have a privacy interest.

23

24

25

So if we were to take Microsoft's reasoning and extend that, that would mean there would be greater privacy

protection in a situation where you're requesting documents 1 2 simply because somebody else holds them, as opposed to in 3 situations where you directly request from that person --4 THE COURT: Right. MR. PAK: -- through any legal process those same 5 documents and that --6 THE COURT: And then you can refer to those line of 7 8 cases that said you lose your right and expectation of privacy 9 when it's held -- in the older cases --MR. PAK: Absolutely. 10 THE COURT: It's held by a third party. 11 12 MR. PAK: Absolutely, Your Honor. 13 THE COURT: Which may have precipitated the Stored Communications Act or at least prompted it. 14 15 MR. PAK: Absolutely, Your Honor. THE COURT: Right. 16 17 MR. PAK: And there's an additional case that we don't actually cite in our brief, but that's also relevant, 18 Fisher versus the United States where certain documents were 19 20 -- for tax defendants were held by the tax defendant's 21 attorneys, which you could describe as someone that would be the holder of their documents, as opposed to a bank that 22 23 they're interacting with. 24 And even there the Court said, look, all that

matters if you're going to send a subpoena or a document

request -- request and the Court has power to do so under the relevant law with respect to subpoenas then the issue there is one of reasonableness.

So if the Second Circuit was distinguishing the <u>Marc</u>
Rich line of cases based on privacy interest, which it says it
doesn't, but it seems -- that seems to be what it's actually
trying to do, that also doesn't make sense because here under
Fisher the relevant standard that would apply is
reasonableness and the process here is imminently reasonable.
We have to get a search warrant backed by a probable cause
before these documents come anywhere.

So the notion that you should distinguish <u>Marc Rich</u> and that line of cases because there's a privacy interest involved just doesn't make sense.

And going back to, sort of, the issue why -- the distinction between in personam and in-rem power matters is because here we're dealing with emails and other stored documents, photographs and other such material that doesn't conform to traditional notions of property.

Now -- and it's not because the information at issue is digital. For example, if you're dealing with electronically stored information, that information typically sits on an item and if there's a search warrant with respect to that not only is the data on the item important, but the facts surrounding the item are as important as well.

For example, you would want to know the device's serial number. You would want to know how it was seized. All of that stuff is relevant. You would have an original piece of evidence.

With emails and the type of data that's at issue here there's no such thing as an original. We just get a copy. The data itself is valuable abstracted from any physical property.

And, therefore, Rule 41 is sort of ill-equipped to deal with that kind of situation because Rule 41 is specifically about personal property, tangible items and things of that nature.

Recognizing this Congress had created the Stored Communications Act which we -- which, as I said before, creates in power -- in personam power over certain providers. And the distinction between the in personam power under the SCA and Rule 41 becomes quite obvious if you look at the jurisdictional questions that both of those types of applications raise.

So under a Rule 41 search warrant, as Your Honor I'm sure is aware, the basic jurisdictional question is is the property to be searched within the geographical reach of this Court, is it in the district in which the Court sits? And that makes sense, obviously, because you're dealing with property.

The SCA has different questions. Right? So when there's an SCA application before the Court the first question is is the warrant that's being applied for directed at a class of individuals that the SCA grants the Court power over? Specifically, electronic communications service providers or remote computer serving providers. That is the type of question that a Court asks itself when it's -- when it's exercising power in personam.

The second question, assuming that the answer to the first is yes, is does the Court otherwise have jurisdiction over the offense under investigation?

And, again, if both of -- if both of the answers to both of those questions are yes, then the Court is a Court of competent jurisdiction under the SCA and, therefore, then has in personam power over the provider here, Google, or some other ECS or RCS.

And it's at this point, Your Honor, that we look to the law on in personam power and apply the statutory canon of construction that Congress is presumed to legislate against the backdrop of longstanding principles of the common law.

In addition, Your Honor -- and I think one of the mistakes that the <u>Microsoft</u> Court makes we had addressed with respect to <u>Marc Rich</u> and <u>Bank of Nova Scotia</u>.

But another problem is that the Court simply says, well look, we're going to look at the SCA and rather than

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

apply this principle or the -- or the common law on in 1 2 personam jurisdiction we're going to say, all right, well the 3 statute uses the term warrant. And that term warrant comes 4 with it certain baggage and that baggage comes in the form of territorial restrictions.

But based on the fact that the power granted by the SCA is in personam it doesn't make sense that that term would be used to import territorial restrictions on the SCA. number one.

Number two, more logically understood, Your Honor, and this makes complete sense, that the use of the term warrant in the SCA is meant to import the probable cause requirement for certain types of data that are covered by the SCA and not any territorial restrictions.

I think the second -- the second reason that the <u>Microsoft</u> Court -- or the <u>Microsoft</u> decision is wrongly decided has to do with what we refer to as the Cybercrime Convention, or the Cybercrime Treaty, or the Budapest Convention which was ratified in 2006.

And I won't go over all the articles and the explanatory report in detail as it's in the brief, but basically Senate has said in 2006, yes, the current law -- the SCA as it exists at the time does exactly what we are arguing that it does. It allows the Court to order a provider properly before it to produce information, regardless of where

that information is held, so long as the provider has control over that information. That's the same test we see coming out of the <u>Marc Rich</u> and the <u>Hay Group</u> and the <u>Gurley</u> (phonetic) line of cases that we discussed before.

And it's also the exact opposite of what the <a href="Microsoft">Microsoft</a> Court says the SCA does. Now, that's relevant for two reasons.

First, is that the treaty is not self-executing.

Right? So the treaty actually imposes on all the countries that signed it, the United States and 48 other countries, to create domestic law.

What does that mean? That means that not only did the Senate -- not only did the United States, but the 48 countries that entered into this treaty, believed that the type of power that we're talking about requires domestic legislation.

So it's really -- it really shows how even if certain -- if certain things may have an impact overseas it doesn't mean automatically that that is an extraterritorial piece of legislation.

And, in fact, that's what <u>RJR Nabisco</u> tells us about the -- the rule -- I'm sorry -- the presumption against extraterritoriality, that it doesn't matter that some conduct occurs overseas. That's not the proper analysis.

The more important point with respect to the treaty,

Your Honor, is that Senate in enacting it, in ratifying it, decided that it didn't need to make any new legislation. The SCA essentially, or the law at the time, covers that. And I've already covered why that's relevant and particularly persuasive even though that occurred post-enactment.

But, in addition to that, Congress did readdress the Stored Communications Act in 2009 after the treaty was ratified. And the same cases that I described before, <u>Bell versus New Jersey</u> and <u>Schor</u> both -- both say that that's okay. You can look at that too.

out there's -- if there's an interpretation of law out there by the agency responsible for that -- in this case it would be the DOJ or the Executive -- and Congress amends the statutes, but then doesn't change that interpretation, that is also persuasive evidence of what Congress intended originally when it first enacted the statute.

The third -- our third point, Your Honor, is with respect to, again, the presumption against extraterritoriality and I believe, Your Honor, you covered a lot of this point.

THE COURT: Yes. I'm glad you're coming to that point. You know, when you look at this your argument so far didn't mention the presumption against extraterritorial application.

And when you look at the lower Court, when you look at Judge Francis and also the Chief Judge, they didn't really

8 9

analyze this problem with that presumption and the Second Circuit took it that way. Do we -- do we have to analyze? This is a question I asked Mr. Hinnen. Do we have to apply the application -- the presumption against extraterritorial jurisdiction? Do we have to go that route? Do we have to look at it that way? Tell me, what's your view on that?

MR. PAK: So I think as Your Honor had pointed out during the questioning is that it is a canon of statutory construction.

THE COURT: Right.

MR. PAK: What I would say is that there are other canons of statutory construction.

THE COURT: But you look at the <u>Morrison</u> case and Justice Scalia said it has to be applied. This is where I had some trouble. It says it has to be applied in all -- any time you're construing Congressional legislation.

Although there are other cases that the Supreme Court said you don't have to necessarily apply canons of statutory instruction. I have the case somewhere here.

Do you have -- do you know what language I'm talking about where Justice Scalia in Morrison --

MR. PAK: Yes.

THE COURT: -- said you've got to apply it in all cases, but then in other cases they suggest -- I'm looking for my outline -- in other cases they suggest it's just merely a

canon of statutory construction and there's cases that say --1 2 wait a minute, hold on for a minute. 3 (Pause in proceedings) 4 THE COURT: Yes, it's Chickasaw Nation versus U.S. 5 they're guides that need not be conclusive. That's the language. Justice Breyer wrote that opinion. 6 MR. PAK: I think -- I think that's correct, Your 7 8 Honor. 9 I will say that because we're very confident that the Morrison -- that the test under Morrison was misapplied by 10 the Second Circuit our position is --11 12 THE COURT: Apply it. 13 MR. PAK: -- even when you apply that --THE COURT: Right. 14 15 MR. PAK: -- they're wrong on that under the sense 16 that this is a domestic application. 17 But I would also say in addition to that we do have other canons of construction and sometimes they interact with 18 each other and one of those is that Congress legislated 19 against the backdrop of common law. 20 21 THE COURT: Right. MR. PAK: In this case a law on the scope of a 22 Court's power in personam to produce documents -- to compel 23 24 someone to produce --

THE COURT: Right.

1 MR. PAK: -- to produce documents.

THE COURT: All right. Let's go to the -- you know, presumption and see how you come out on that.

MR. PAK: Yes, Your Honor.

So with respect to the second step, the focus of Section 2703, as Your Honor had mentioned before, we think that the <u>Microsoft</u> Court was incorrect in looking at the statute as a whole.

And when it did get to Section 2703 it was also incorrect in concluding that the focus of that was privacy.

There's nothing -- privacy does not occur -- there's no reference to privacy at all in that section.

THE COURT: Right.

MR. PAK: The title of the section is required disclosure of customer communications or records.

Every subsection under 2703 leads to the same result and governs the same process which is the fact -- the circumstances or the conditions that the Government must meet in order to compel disclosure in response to legal process. It's all about disclosure.

Now, even if it impacts privacy and even if that was perhaps the underlying goal of creating the statute, that's not relevant under <u>Morrison</u>. <u>Morrison</u> says you look at the statute and you determine how it functions. What is the conduct that it seeks to regulate, regardless of what longer

term goal it may have or overarching goal, what is the focus?

What is the conduct being regulated?

Here that conduct is compelled disclosure or required disclosure and that occurs in the United States. I don't think there's any dispute about that.

THE COURT: What about the -- Google's argument that
-- and I guess bolstered by the Second Circuit -- that it's
the actual retrieval when they -- whatever they do when they
press the button in the computer in the U.S. they actually
retrieve it and that's the actual extraterritorial
application? Can you talk about that and where does
disclosure occur?

MR. PAK: Absolutely, Your Honor.

So, first off, the disclosure occurs in the United States.

The fact that -- and I think the Second Circuit described the process of retrieval in the context of saying -- after it had concluded that privacy was the focus on Section 2703. We disagree with that, obviously, but let's assume that that were the case.

Let's assume that the focus were privacy. Our position is that even if the data originally sat overseas in a foreigner server controlled by the provider, the invasion of privacy, if that's the concern of the statute, occurs at two different or three different points.

One, when an application is made and approved by a Court for a particular warrant -- an SCA warrant. At that point there's a decision made that the -- that documents can be looked at.

Number two is when the documents are disclosed to the United States. That occurs in the United States.

But, most importantly, the invasion of privacy would occur when somebody has eyeballs on the data. It's when somebody's looking email by email, document by document, and saying, hey, this is -- this is just personal stuff, this is evidence of the specified Federal offenses and that undoubtedly occurs in the United States.

And the application of Attachment 2 -- of Attachment B(2) which identifies what the Government can actually look for and seize is all done by Federal agents and law enforcement officers, not by the providers.

So the fact that there's a retrieval of data that is copied from a location overseas doesn't really -- doesn't really trigger those types of concerns.

But, again, we also think that the focus -- to say that 2703 is focused on privacy is also an incorrect application of <a href="Morrison">Morrison</a>.

And, finally, with respect to that same point, again, the notion that privacy matters, even if it did, it still wouldn't impact the argument because at the end of the

day even if privacy was a concern and even if the Second

Circuit was focused on the Fourth Amendment -- again,

reasonableness is a requirement or a warrant is a requirement

because warrants are reasonable when they're approved by a

neutral and detached Magistrate.

Both of those options -- both of that occurs here, right? So not only is it reasonable to say the provider has to produce information, but if it's sensitive you have to get a warrant first. That's reasonable.

But also it involves a warrant that a Judge looks at

-- in this case Your Honor -- to establish -- to assess

whether probable cause -- the probable cause standard has been

met.

I want to move on to our fourth point, our last point, as to why we think this -- this decision is incorrect.

And this is another canon of statutory construction which is to say if you have a reasonable reading of a statute you shouldn't -- you shouldn't take another reading that leads to absurd results and here we have absurd results.

Nothing in the SCA suggests that there's certain data that's off limits completely.

But what we have here is a situation where in this case we get a search warrant -- we get a warrant under the SCA. There are emails that we don't get or email content in the form of attachments or photographs or whatever the

situation may be and there's no way for us -- for us to 1 2 actually get that information under Microsoft. 3 Now, Microsoft says, well, we think the better 4 process is to use international process like an MLAT, Mutual 5 Legal Assistance Treaty request, or some other process, but that doesn't work here under the facts of -- of this case. 6 Under stipulation, paragraph number four, Google 7 8 stipulates that the country or countries in which specific 9 user data or components of that data is located may change. 10 It is possible, therefore, that the network will change the location of data between the time when legal process is sought 11 12 and when it is served. That is a very narrow window of time. 13 And just to draw a picture of what that could look like is -- is somebody's on the phone with Google and says, 14 15 okay, you know, here are the five countries where you have some data. You hang up, you're about to go seek process and 16 17 it's gone. 18 THE COURT: All right. MR. PAK: It moves around to another location. 19 THE COURT: I guess you can have an order every 20 21 day --22 MR. PAK: Yes. 23 THE COURT: -- from a Judge --24

MR. PAK: Exactly.

25

THE COURT: -- to Google requiring them to search

Pak - Argument every day. 1 2 MR. PAK: Exactly. 3 THE COURT: I'm not being facetious. 4 MR. PAK: No. 5 THE COURT: Go ahead. MR. PAK: And -- and the bigger problem, Your Honor, 6 is that we don't even -- we can't even say with certainty 7 8 which country the data's in, as has come out in the 9 stipulations as well as in your exchanges with Google's 10 counsel and so an MLAT is impossible. 11 But let's say that an MLAT were possible. Let's say 12 by some miracle or let's just assume away that problem and say Google can tell us that all the data is in Ireland, for 13 14 example. 15 THE COURT: Right. 16 MR. PAK: We would then have to go to Ireland 17 through an MLAT and have them seek the data. They would go to Google and then Google would say 18 well there's no one here that can actually retrieve that data, 19 20 you have to go back to the U.S. 21 They would come back to us and it's sort of like --I mean, it's a circular problem. It's one that doesn't go 22

THE COURT: Right.

23

24

25

away --

MR. PAK: -- because we'd be stuck with the

Microsoft decision.

THE COURT: Right.

MR. PAK: But, again, that is an absurd result.

What's even more absurd is if you step back for a second and think about the big picture. You have a situation here with U.S. victims, a U.S. target and conduct that primarily occurs in the United States.

Google would be able to retrieve all the emails or all the other data that we request in the search warrant in the U.S.

The targets would be able to do the same.

The only people that would have no access to that information would the United States and this is after a showing of probable cause that the information relates to the specified -- to a certain set of Federal offenses.

And the other problem is if we're talking about extraterritoriality and concerns about comity I think we've addressed the fact that -- Your Honor's addressed with the Google's counsel that practically that doesn't really make sense because even Google doesn't know where specific data is held at any given point in time with certainty.

THE COURT: You know, the one question I had is -- maybe this may be better addressed to Google.

Your position is since this is an in personam order that had you used a subpoena and the data was older than 180

3

4 5

6

7 8

9

10

11

12

13

14 15

16

17

18

19

20

21

22

23

24

25

days there's no question under the Stored Communications Act they'd be required to produce it.

But because it's a warrant and using the Second Circuit's ruling, you can't get it even though a judicial officer, you know, approved it.

So the protection for privacy is even greater because you had a judicial officer looking and there was a showing of probable cause.

What reason would Congress make to make a distinction like that to say, okay, you can't get this -- you can't get the information because it's stored overseas even though you got a Judge to a look at it, even though you showed probable cause, but you can get it with merely issuing a subpoena without a Judge and with probable -- what -- what distinction -- I know this probably should be addressed to Google because you're going to say there's no distinction, but what -- what basis would there be for Congress to come up with such an irrational distinction?

MR. PAK: Your Honor --

THE COURT: The only --

MR. PAK: -- I can't think of one that makes sense.

THE COURT: And I think the only way you wiggle out of that is maybe what the Second Circuit did, and respectfully, is they didn't address that. I mean, they just didn't address that Marc Rich argument --

MR. PAK: That's right. 1 2 THE COURT: -- because that was a difficult argument 3 to try to -- to cope with. MR. PAK: That -- that's correct, Your Honor. 4 THE COURT: Because it makes it totally irrational. 5 MR. PAK: That's correct. That's correct, Your 6 Honor. 7 8 THE COURT: Is there anything in legislative history 9 that talked about distinguishing between --MR. PAK: Making it easier to get data --10 THE COURT: Yes. Other than --11 12 MR. PAK: -- by subpoena? THE COURT: Other than, I guess, Congress felt that 13 because it was more current data, it was within 180 days and 14 15 more live data, so to speak, they wanted to make sure that a 16 Judge looked at it and there was probable cause. 17 Is there any other reason why, in the statute, why they -- they required a Judge to look at it? 18 MR. PAK: I -- I don't think so. 19 20 I would point out just one -- just one note and I 21 don't think that this changes the analysis in any way. Under 2703(b) if you use a subpoena notice is automatically provided 22 23 to --24 THE COURT: Right. 25 MR. PAK: -- or you have to --

Pak - Argument THE COURT: Right. 1 2 MR. PAK: -- provide notice. 3 THE COURT: That's right. You're right. Yes. 4 MR. PAK: But -- but at the same time the notion that -- which is essentially what Microsoft holds -- the 5 notion that subpoenas can have extraterritorial reach, whereas 6 things backed by warrants cannot, because it's focused on 7 8 privacy, when warrants provide the highest level of protection 9 of privacy that is offered under the American Judicial System 10 just doesn't -- doesn't really make sense. It's -- it doesn't only lead to absurd results, but it's just sort of a very 11 12 strange reading of what the SCA does. And to the extent that privacy -- that concerns 13 about privacy undergirded that analysis which Judge Lynch had 14 15 pointed out, this is not really about privacy. 16 And to the extent that it was, again, we would be 17 fine --18 THE COURT: Yes. MR. PAK: -- under the Fourth Amendment. 19 20 THE COURT: It appears if this case went to the 21 Circuit -- this case that we have before us -- Judge Lynch would definitely be on the side of the Government. I mean, 22 23 that's my read.

I can't -- read -- reread that concurring opinion and, you know, he basically said this is not the situation

24

1 that's now before this Court.

MR. PAK: Yes. I think -- I think the one thing, as Your Honor noted in reviewing the <u>Microsoft</u> Court, is they didn't think about the Budapest Convention.

THE COURT: Yes.

MR. PAK: And I know Judge Lynch was looking for something because it was very close, at least --

THE COURT: Right.

MR. PAK: -- when you read his analysis -- looking for something to say, look, Congress may have wanted this. So he didn't have the benefit of looking at the Budapest Convention.

THE COURT: Right.

MR. PAK: Or their case law that says that that kind of post-enactments action by Congress can be relevant, so I think it would make a difference. I think it would make a difference.

I'd also make the point that if we're talking about concerns about comity and extraterritoriality and sort of imposing on sovereign states, even when you don't have a U.S. target, which we -- which we have here, but even if you didn't have a U.S. target or defendant one of the -- as I said before, the second jurisdictional question that generally applies for Stored Communication Act warrants is that the Court needs to have jurisdiction over the offense.

And a lot of concern about, hey, well, is Congress regulating conduct that occurs overseas is handled by the fact that the Court, at least in cases where you're -- where you're outside of, for example, Google's district, needs to know that, look, do I have jurisdiction over the offense?

And, as Your Honor is aware, U.S. Courts can have jurisdiction over offenses, part of which occur overseas, or involve actors overseas especially in this day and age where you hear stories and cases about hacking into United States infrastructure or companies.

So we think all of those concerns really don't apply.

We think that we're good under the Fourth Amendment.

We're good under the Stored Communications Act that interpreting the SCA in the way that <u>Microsoft</u> does simply leads to absurd results.

I'd also like to point out that -- that we think that the -- Your Honor -- whatever Your Honor decides it should be fully engaging on the <u>Microsoft</u> opinion as opposed to the specific facts of this case.

Because, as we have pointed out before, look,

Microsoft has their way of storing data. Google has their way

of storing data. It's not for me to say certainly which is

better.

I think in the stipulations their -- their network

architecture is referred as state of the art and I have no 1 2 reason to think that's not true, but to then have a ruling 3 that is specific to network architecture creates problems. 4 Not only does it create, for example, attacks on Google if 5 this case were -- if a ruling would only apply to Google as opposed to on Microsoft, but it also creates a problem of the 6 need for judicial inquiry into the ever-changing network 7 8 architecture of providers or new providers --9 THE COURT: Right. MR. PAK: -- that come into the marketplace. 10 THE COURT: Well, whatever I do it's not going to be 12 the last word.

MR. PAK: That may be true, Your Honor.

THE COURT: You know the Third Circuit's going to get this and probably the Supreme Court. They don't get the Second Circuit case, but, okay.

Let me just see if I have any questions for you, Mr. Pak.

MR. PAK: Yes.

11

13

14

15

16

17

18

19

20

21

22

23

24

25

(Pause in proceedings)

THE COURT: Are there any -- I know I may have asked you this, but are there any cases under the Stored Communications Act which address the power of the Court to issue a subpoena to require disclosure of information that's held overseas? You know, under a subpoena. That whole issue

that I didn't, so if it's okay with Your Honor I'll stretch my legs and come up to the podium --

THE COURT: Sure.

21

22

23

24

25

MR. HINNEN: -- for my brief response.

THE COURT: Okay.

MR. HINNEN: Just a couple of points that I'd like

1 to address, Your Honor.

First is that a patchwork of inconsistent laws in different jurisdictions is not -- is not favorable to anyone.

THE COURT: Right.

MR. HINNEN: It's difficult for the Government, the providers, users and the Courts.

And in addition to creating uncertainty it creates the potential for forum shopping and it will also create the necessity for me to meet Mr. Pak in courtrooms across the country.

THE COURT: 25,000 cases.

MR. HINNEN: Exactly. And have a -- since we're in Pennsylvania, Your Honor, have a sort of Groundhog Day moment in which we repeat the same argument over and over again.

Second, I think that the Second -- if you look carefully at the Second Circuit it did refer to the canon that interpretation of a statute may be informed by existing common law rules.

It's just that when it looked at it the common law that it found relevant was the common law applicable to search warrants, not to in personam jurisdiction. Something that's not used or referred to anywhere in the statute.

And it was part of its reliance on that common law understanding of how warrants were to be applied and how that

J

8 9

THE COURT: Yes.

25 MR. HII

had ultimately been codified in rules in the United States that -- that resulted in it ruling the way it did.

I don't think Google would take issue with the fact that -- that Judge Lynch was right, this is not about privacy. And when I say that I say, you know, the rule that a U.S. warrant can't be used to get data stored overseas is not about privacy, except in the sense that I think it may reflect the decision that each sovereign is entitled to determine the rules that apply to -- for Government agencies to obtain access to private property that's within their jurisdictions.

And so while it may not be about U.S. privacy, it may be about the ability of different sovereigns to determine the privacy rules that are going to -- that are going to apply in their jurisdictions.

I would caution the Court against making the assumption that Congress was being sneaky or clever. In my experience -- and I worked for Congress for a little while -- that's rarely the case.

And you heard Mr. Pak say several times the Second Circuit was looking -- if they were looking for something to hang their hat on -- it shouldn't be a matter for looking something. They're -- the statute is clear. It's even clear about geographic location and how it applies --

MR. HINNEN: -- with respect to geographic location.

It says it applies outside the district whereas a search 1 2 warrant would traditionally apply only inside the 3 jurisdiction. 4 Notably, it doesn't say it applies outside the 5 country, even though a search warrant would ordinarily. THE COURT: I don't know if you had a chance to 6 watch any of the hearings on the confirmation of the Attorney 7 8 General, but they asked him about -- there's apparently a bill 9 that Senator Hatch just sponsored --10 MR. HINNEN: That's correct. THE COURT: -- to address some of these issues, so 11 12 they asked Senator Sessions about it, but she didn't know anything it, but he said we'd look into it, but --13 MR. HINNEN: Yes. 14 15 THE COURT: Anyway, it's interesting. 16 MR. HINNEN: Yes. 17 THE COURT: Go ahead. MR. HINNEN: No, I agree. 18 19 THE COURT: Yes. 20 It is very interesting. MR. HINNEN: 21 Just one or two more points. I don't think there's anything absurd about thinking 22 that a warrant issued in the United States shouldn't be 23 24 compelled to conduct a search or seizure overseas.

And Your Honor has pressed both me and Mr. Pak on

Hinnen - Argument well where does the conduct actually occur? It's a process. 1 2 There's several steps in it. 3 And the receipt of the warrant occurs in the United 4 States. The search occurs in the data center -- the Second 5 Circuit found the search occurs in the data center where the 6 data is. 7 8 The seizure occurs in the data center where the data 9 is. And the disclosure occurs here in the United States. 10 I guess the other thing I would say --11 12 THE COURT: I guess that -- I know Judge Francis cited Professor Kerr's article that talked about a search of 13 electronic data actually occurs when it's -- when it's 14 15 uploaded or retrieved or when it's disclosed. If you read his Lower Court opinion he cited 16 Professor Kerr who said this is when a search happens in the 17 data world. 18 19 MR. HINNEN: Yes. THE COURT: Which was different than what the Second 20 21 Circuit ultimately retrieved. Kerr doesn't see the search as 22

occurring when they retrieve it, as opposed to when it's actually -- I'm going to call uploaded or downloaded or whatever the terminology is, but actually disclosed.

23

24

25

MR. HINNEN: Agreed, Your Honor. I think there --

Case 2:16-mj-00960-JS Document 30 Filed 02/14/17 Page 66 of 74 Hinnen - Argument there are disputes about that. 1 2 THE COURT: The definition of the search in the data 3 world? 4 MR. HINNEN: Yes, and then different commentators 5 come out --THE COURT: Right. 6 MR. HINNEN: -- in different places. 7 8 And just to sort of bring us full circle here. 9 THE COURT: Right. MR. HINNEN: You know, the Budapest Convention is a 10 100 page kind of statutory monster. 11 12 The Stored Communications Act is a terse 12 or 13 13 pages long. And the obligation to enable the production of -- of 14 15 documents by providers in your territory is one very, very, very, very, very small part of that Budapest Convention. 16 Again, to kind of suggest that rather than just say 17 in the Stored Communications Act this was intended to apply 18 overseas data as well, that Congress expressed that intent 19 20 through a very small provision in a 100 page treaty that it 21

ratified 20 years after the passage, it's doing a lot more work than ought to be necessary with respect to a short, plain statute.

And I think what we're left with at the end of the day is the sense that this is a very complex issue.

22

23

24

THE COURT: Right. I agree with you.

MR. HINNEN: It affects a lot of providers. It affects a lot of different stakeholders. It affects the U.S. Government. It affects -- it has the potential to affect foreign Governments.

It's not clearly spoke to by the existing statute. Senate Hatch is -- is one among many senators who have put forward proposals. The Department, I know, has looked at and evaluated them. The providers have looked at and evaluated them and that's the -- that's the way forward here.

I know that doesn't -- doesn't help us resolve this particular matter, but engaging in sort of hermeneutic gymnastics in able to -- in order to find clarity in a statute that doesn't clearly address this particular issue or a set of facts I think is -- is the wrong approach.

And the right approach is for Congress to address all of these various complex policy issues, to hear from all of the stakeholders and to actually pass law on the -- on the subject.

THE COURT: I guess that's true.

But on the other hand you can see where for years IP providers have been -- Internet providers have been given this information and from the Government's perspective this aberration called <a href="Microsoft">Microsoft</a> case came along and threw everything in chaos, so, you know, they see it -- they see it

```
otherwise.
 1
 2
               But I completely -- you know, I completely
 3
     understand your argument. Thank you.
 4
               MR. HINNEN: Thank you, Your Honor.
               THE COURT: Okay. Is there anything else from the
 5
     Government?
 6
 7
               MR. LEVY: Your Honor, the only -- the only
 8
     outstanding footnote, I guess, here is the non-disclosure --
 9
               THE COURT: Right.
10
               MR. LEVY: -- order.
               With respect to 16-960-M-1 I think we signaled in
11
12
     our brief that there was a way to resolve that one.
13
               THE COURT: Yes, go ahead. I'd like to resolve it
14
     because --
15
               MR. LEVY: Yes, but the --
16
               THE COURT: -- I'd like to spend the time on these
17
     really important issues rather than this.
               MR. LEVY: But the problem is with regard to the
18
     other matter which is --
19
20
               THE COURT: How do we resolve the 1061, Mr. Levy?
21
               MR. LEVY: In 960-M-1.
22
               THE COURT: 960, I'm sorry.
               MR. LEVY: Well, in that one the subject knows he's
23
     under investigation.
24
```

THE COURT: Which one?

MR. LEVY: We're not worried about him destroying 1 2 other evidence that he has in his possession. THE COURT: Which one? 3 4 MR. LEVY: 960-M-1. 5 THE COURT: Okay. MR. LEVY: And so the only concern is will he 6 destroy evidence that's on Google's servers? 7 8 If Google can tell us that no matter where it is 9 they'll preserve it pending the results -- the results of this 10 litigation we're -- we don't have a problem with them telling the customer. 11 The alternative is for the Court to continue it 12 13 until this litigation is over. Either way it takes care of the Government's concern 14 15 that evidence that Google maintains would be destroyed because 16 we -- we don't have a basis to argue that with respect to 17 things on his own computer. THE COURT: You know, my suggestion -- and this is 18 19 like kind of an attempt to settle this little small dispute --20 is to -- you know, can the Government live with a date like a 21 couple of years out? 22 MR. LEVY: Yes. THE COURT: And just -- and then hopefully, Mr. 23 24 Hinnen, you can say okay that's fine for this problem unless

you want to make a statement and you want, you know, to make a

70 Colloquy profound statements that's going to apply to every one of your 1 2 cases, but I think there's bigger fish to fry here. 3 And I don't really want to spend all of my time 4 dealing with this one when I can say, okay, I'll sign an 5 amended order, make it two years, or whatever year you guys 6 can agree on. 7 And then, you know, come back to me if you need 8 further non-disclosure --9 MR. LEVY: If we need to extend it we can. THE COURT: -- on this particular case. 10 MR. HINNEN: Yes, Your Honor. I think if it comes 11 -- if what we're seeking here is agreement of the parties I 12 13 need to consult my party. THE COURT: Okay. 14 15 MR. HINNEN: On the other hand, I think if the Court were to issue an order of the type the Court is describing I 16 17 think it's somewhat unlikely that --18 THE COURT: Okay. 19 MR. HINNEN: -- my client would come back and challenge that order. 20 21 THE COURT: Right. Because you made that clear in your papers. You weren't challenging the right -- at least in 22

this case you weren't challenging the right of the Government to seek a non-disclosure order. It was more the length of the -- the length of it.

23

24

MR. HINNEN: That's correct. 1 THE COURT: So, okay. All right. I can deal with 2 3 that, I think. Okay. Thank you. And on the -- and, Mr. Levy, just on the position on 4 the -- is that -- am I right that Google only argued the 5 overbreadth in one of the warrants? 6 7 MR. LEVY: That's correct, Your Honor. 8 THE COURT: Was there --9 MR. HINNEN: Yes, that is. THE COURT: Is there a distinction in what you asked 10 for between the warrants? 11 12 MR. LEVY: I think there is. 13 THE COURT: Oh, there is. MR. LEVY: Yes. 14 15 THE COURT: Okay. All right. MR. LEVY: Google sought overbreadth in one and not 16 17 in the other. THE COURT: Okay. All right. Okay. Well, thank 18 19 you very much. Obviously, this is important. I'll get this 20 out as soon as I can and I appreciate, you know, all the 21 effort you showed today. Thank you very much. 22 MR. LEVY: Your Honor, before we finish. You had asked about sealing the transcript? 23 24 THE COURT: Oh, yes. 25 MR. LEVY: I don't think anything was said here

Colloquy

And I would propose that, obviously,, we need to talk 1 today. 2 to Google about it. 3 But I don't think with the exception of one attachment to one pleading that any of the pleadings contain a 4 5 citation to any of the accounts. I think there's an attachment that the production letter on one that he's 6 attached to thing as --7 8 MR. PETKUN: That's right. All of the exhibits, I 9 think, have the hash values and the algorithms that pertain to 10 specific -- they give away the specific target accounts for both of the two cases, but other than those attachments to 11 12 Google's --13 THE COURT: It's not in the transcript? MR. PETKUN: Right. 14 15 MR. LEVY: No, but what I was going to suggest, and we, obviously, need to work on a stipulation for this, but I 16 17 think that if we can agree on redactions we could agree to the unsealing of the pleadings, not the search warrant and the 18 affidavit, but the pleadings themselves --19 20 THE COURT: Okay. 21 MR. LEVY: -- in this case. THE COURT: Yes, that's fine. Okay. You want to 22 23 submit something to me, Mr. Levy? 24 MR. LEVY: Yes, we'll work out an agreement --

THE COURT: Okay.

MR. LEVY: -- and get something to you. 1 2 THE COURT: And I'm going to order this transcript 3 on an expedited basis, but I won't seal it and, obviously, 4 both sides will get copies. 5 MR. LEVY: Great. THE COURT: Okay. What's the status, by the way, 6 with the Second Circuit? Anything going on with that 7 rehearing petition? 8 9 MR. PAK: Your Honor, the petition for rehearing is 10 still pending. 11 THE COURT: It's been pending for awhile, right? 12 MR. PAK: Yes, Your Honor. THE COURT: Yes. Okay. All right. Thank you very 13 14 much. 15 ALL COUNSEL: Thank you, Your Honor. 16 (Proceedings concluded at 2:17 p.m.) 17 18 CERTIFICATION 19 20 I, Joan Pace, court approved transcriber, certify that the foregoing is a correct transcript from the 21 official electronic sound recording of the proceedings in the 22 23 above-entitled matter. 24 25 January 20, 2017